LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 7

(*Footprinting* dan *Scanning*)

DISUSUN OLEH

Indah Sekar Ningrum (21/478139/SV/19241)

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

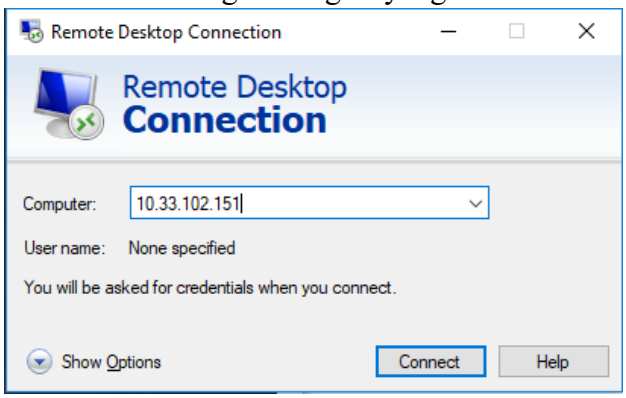
2023

A. Link Github

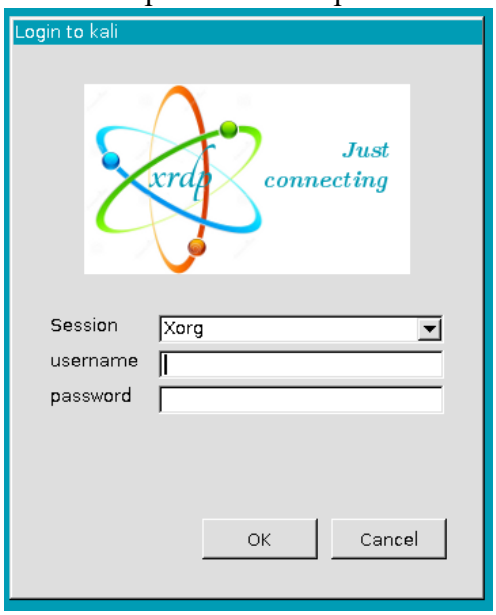
https://github.com/indah0503/Praktikum-Keamanan-Informasi-Kelas-A/tree/Pertemuan-7

B. Footprinting dan Reconnaissance

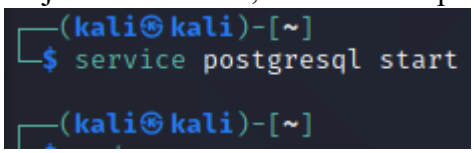
1. Jalankan mesin Kali Linux dengan Remote Dekstop Connection di PC windows. Masukkan masing-masing IP yang sudah di sediakan.



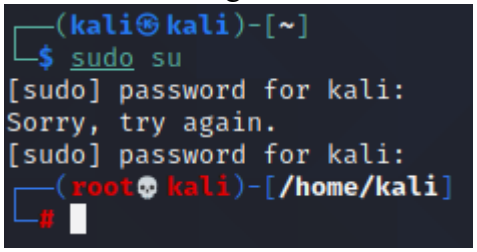
2. Masukkan password **kali** pilih username **kali**.



3. Desktop Kali Linux muncul, klik ikon Terminal.
4. Di jendela terminal, ketik service postgresql start dan tekan Enter.



5. Masuk akun sebagai root, ketik sudo su masukkan password : kali.



6. Ketik msfconsole dan tekan Enter. Tunggu hingga Metasploit Framework diluncurkan.

```
┌──(root💀kali)-[/home/kali]
└─# msfconsole
```

```
       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>

msf6 >
```

7. Di baris perintah msf, ketik db_status dan tekan Enter. Jika Anda mendapatkan postgresql yang dipilih, no conecction, maka database tidak dimulai.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
```

8. Jika Anda mendapatkan postgresql terhubung ke pesan msf, lewati ke Langkah 13.
9. Keluar dari metasploit dengan mengetik exit dan tekan Enter.
10. Untuk menginisialisasi database ketik msfdb init dan tekan Enter.
11. Sekarang restart layanan postgresql dengan mengetik service postgresql restart.
12. Luncurkan kembali kerangka kerja metasploit dengan mengetik msfconsole dan tekan Enter. Tunggu hingga kerangka metasploit dimulai dan memberi Anda baris perintah msf.
13. Periksa kembali apakah databse terhubung ke metasploit dengan mengetik db_status dan tekan Enter.
14. Ketik nmap -Pn -sS -A -oX Test 10.33.102.0/24 dan tekan Enter. Dibutuhkan sekitar 10 menit bagi namp untuk menyelesaikan pemindaian subnet.

```
msf6 > nmap -Pn -sS -A -oX Test 10.33.107.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.33.107.0/24

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 20:45 CDT
```

15. Setelah selesai, Anda akan mendapatkan pesan Nmap done dengan nmap yang menunjukkan jumlah total host yang aktif di subnet.

```
Nmap scan report for 10.33.107.48
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows 10 Pro 15063 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-PD7QHPL
| Not valid before: 2023-01-24T08:45:25
|_Not valid after:  2023-07-26T08:45:25
|_ssl-date: 2023-03-28T02:47:09+00:00; +20m20s from scanner time.
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 2 hops
Service Info: Host: DESKTOP-PD7QHPL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h24m29s, deviation: 3h29m38s, median: 20m19s
| smb-os-discovery:
|   OS: Windows 10 Pro 15063 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-PD7QHPL
|   NetBIOS computer name: DESKTOP-PD7QHPL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-28T09:42:11+07:00
| smb-security-mode:
```

16. Ketik db_import Test dan tekan Enter untuk mengimpor hasil pengujian.

```
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.11.1'
[*] Importing host 10.33.107.122
[*] Importing host 10.33.107.123
[*] Importing host 10.33.107.124
[*] Importing host 10.33.107.125
[*] Importing host 10.33.107.126
[*] Importing host 10.33.107.127
[*] Successfully imported /home/kali/Test
```

17. Ketik host dan tekan Enter untuk menampilkan host dan detailnya seperti yang dikumpulkan oleh nmap.

```
msf6 > host
[*] exec: host

Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] [-p port] hostname [server]
       -a is equivalent to -v -t ANY
       -A is like -a but omits RRSIG, NSEC, NSEC3
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -p specifies the port on the server to query
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -U enables UDP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
```

18. Ketik db_nmap -sS -A 10.33.107.84 dan Enter.

```
msf6 > db_nmap -sS -A 10.33.107.84
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 20:46 CDT
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 3.60 seconds
```

19. Nmap memindai mesin dan memberi Anda detail layanan yang berjalan di mesin. Ini adalah bagaimana Anda dapat menemukan layanan pada masing-masing mesin.
20. Untuk mendapatkan informasi layanan dari semua komputer aktif di jenis subnet ketik services dan tekan Enter.

```
msf6 > services
Services
========

host  port  proto  name  state  info
----  ----  -----  ----  -----  ----
```

21. Ketik use scanner/smb/smb_version dan tekan Enter untuk memuat modul pemindai SMB.

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) >
```

22. Kemudian ketik show options dan tekan Enter untuk menampilkan opsi konfigurasi yang terkait dengan modul.

```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

23. Ketik set RHOSTS 10.33.107.8-16 and press Enter. Kemudian ketik set THREADS 100 dan tekan Enter. Untuk menampilkan opsi konfigurasi yang terkait dengan modul ketik run dan tekan Enter.

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.33.107.8-16
RHOSTS ⇒ 10.33.107.8-16
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS ⇒ 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.33.107.8-16:       - Scanned 2 of 9 hosts (22% complete)
[*] 10.33.107.8-16:       - Scanned 5 of 9 hosts (55% complete)
[*] 10.33.107.8-16:       - Scanned 8 of 9 hosts (88% complete)
[*] 10.33.107.8-16:       - Scanned 9 of 9 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

24. Ketik hosts dan tekan Enter. Sekarang kamu dapat melihat bahwa informasi os_flavor sudah dikumpulkan dan ditampilkan pada potongan layar.

```
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address  mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------  ---  ----  -------  ---------  -----  -------  ----  --------
```

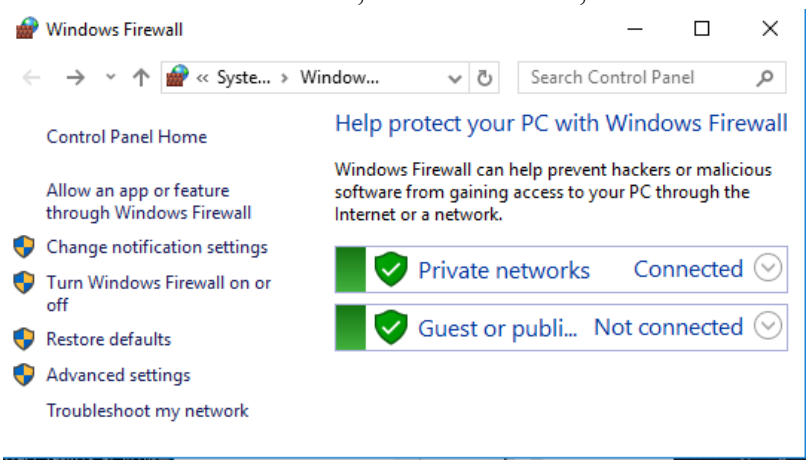
C. Teknik Pemindaian Jaringan

1. Ketik perintah nmap -sT -T3 -A 10.33.107.22 (IP PC windows) dan tekan Enter untuk melakukan TCP Connect Scan pada Windows machine.

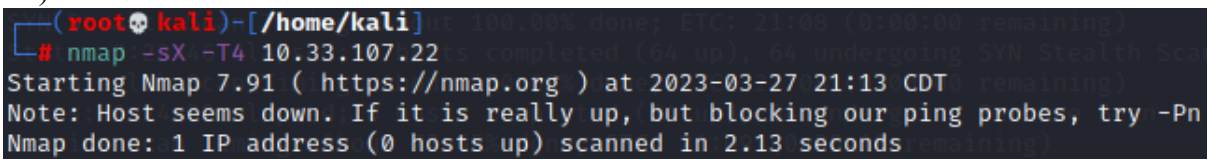
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sT -T3 -A 10.33.107.22
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 20:58 CDT
Nmap scan report for 10.33.107.22
Host is up (0.014s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows 10 Pro 15063 microsoft-ds (workgroup: WORKGROUP)
1521/tcp open  oracle-tns   Oracle TNS listener 1.5.0.0.0 (unauthorized)
3306/tcp open  mysql        MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 2 hops
Service Info: Host: DESKTOP-AIVUJRL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h59m46s, deviation: 4h02m28s, median: 20m12s
|_nbstat: NetBIOS name: DESKTOP-AIVUJRL, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:37:14:4b (Quanta Computer)
| smb-os-discovery:
|   OS: Windows 10 Pro 15063 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-AIVUJRL
|   NetBIOS computer name: DESKTOP-AIVUJRL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-28T09:18:32+07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
```

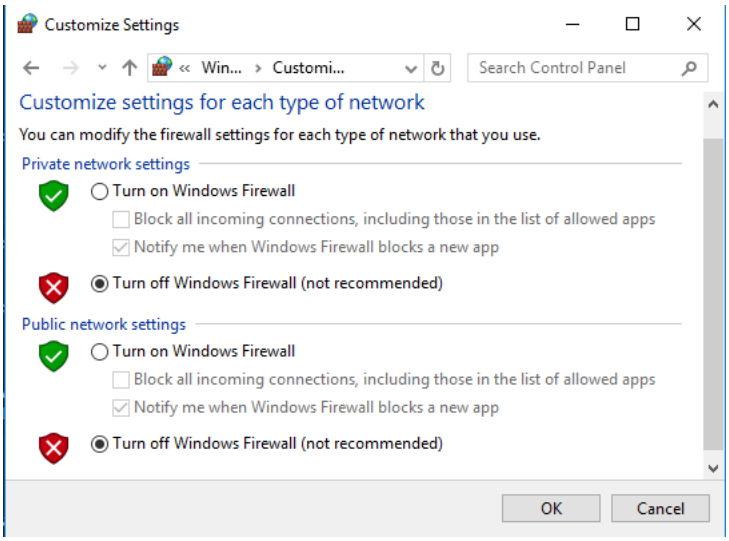
2. Beralih ke mesin Windows , masuk ke mesin, dan aktifkan Windows Firewall.



3. Beralih kembali ke mesin Kali Linux. Ketik nmap -sX -T4 10.10.10.12 di command prompt dan tekan Enter untuk melakukan pemindaian Xmas dengan waktu agresif (-T4).



4. Beralih ke mesin Windows dan matikan Windows Firewall.



5. Beralih kembali ke mesin Kali Linux. Ketik nmap -sA -v -T4 10.10.10.12 di terminal baris perintah.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sA -v -T4 10.33.107.22
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:15 CDT
Initiating Ping Scan at 21:15
Scanning 10.33.107.22 [4 ports]
Completed Ping Scan at 21:15, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:15
Completed Parallel DNS resolution of 1 host. at 21:15, 0.00s elapsed
Initiating ACK Scan at 21:15
Scanning 10.33.107.22 [1000 ports]
Completed ACK Scan at 21:15, 1.44s elapsed (1000 total ports)
Nmap scan report for 10.33.107.22
Host is up (0.00064s latency).
All 1000 scanned ports on 10.33.107.22 are unfiltered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
           Raw packets sent: 1123 (44.912KB) | Rcvd: 1242 (50.382KB)
```

6. Ketik perintah nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12, dan tekan Enter.
   Firewall mati

```
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn -p 80 -sI 10.33.107.23 10.33.107.22
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:40 CDT
Idle scan using zombie 10.33.107.23 (10.33.107.23:80); Class: Incremental
Nmap scan report for 10.33.107.22
Host is up (0.23s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.14 seconds
```

   Firewall nyala

```
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn -p 80 -sI 10.33.107.23 10.33.107.22
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:44 CDT
Idle scan using zombie 10.33.107.23 (10.33.107.23:80); Class: Incremental
Nmap scan report for 10.33.107.22
Host is up (0.20s latency).

PORT   STATE           SERVICE
80/tcp closed|filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds
```

7. Di jendela terminal, ketik nmap -sP 10.33.107.* dan tekan Enter untuk memindai seluruh subnet untuk sistem yang hidup.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sP 10.33.107.*
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:42 CDT
Nmap scan report for 10.33.107.21
Host is up (0.0010s latency).
Nmap scan report for 10.33.107.22
Host is up (0.00099s latency).
Nmap scan report for 10.33.107.23
Host is up (0.00067s latency).
Nmap scan report for 10.33.107.25
Host is up (0.00063s latency).
Nmap scan report for 10.33.107.26
Host is up (0.00071s latency).
Nmap scan report for 10.33.107.28
Host is up (0.00072s latency).
Nmap scan report for 10.33.107.30
Host is up (0.00083s latency).
Nmap scan report for 10.33.107.34
Host is up (0.00068s latency).
Nmap scan report for 10.33.107.35
Host is up (0.00066s latency).
Nmap scan report for 10.33.107.37
Host is up (0.00061s latency).
Nmap scan report for 10.33.107.39
Host is up (0.00056s latency).
Nmap scan report for 10.33.107.40
Host is up (0.00065s latency).
Nmap scan report for 10.33.107.41
Host is up (0.00082s latency).
Nmap scan report for 10.33.107.42
Host is up (0.00070s latency).
Nmap scan report for 10.33.107.43
Host is up (0.00069s latency).
Nmap scan report for 10.33.107.44
Host is up (0.00083s latency).
Nmap scan report for 10.33.107.48
Host is up (0.00066s latency).
Nmap scan report for 10.33.107.105
Host is up (0.0021s latency).
Nmap scan report for 10.33.107.106
Host is up (0.0021s latency).
Nmap scan report for 10.33.107.252
Host is up (0.00055s latency).
Nmap scan report for 10.33.107.254
Host is up (0.00032s latency).
Nmap done: 256 IP addresses (21 hosts up) scanned in 85.84 seconds
```